



General Assembly

Distr.: General
17 September 2007

Original: English

Sixty-second session

Item 95 of the provisional agenda*

**Developments in the field of information and
telecommunications in the context of international security**

Developments in the field of information and telecommunications in the context of international security

Report of the Secretary-General

Addendum

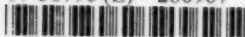
II. Replies received from Governments *(continued)*

Bangladesh

[Original: English]
[29 June 2007]

The world has achieved considerable progress in developing and applying the latest information technologies, which provides a great opportunity for the development of civilization by the circulation of information in the global community. But information technologies can be used by terrorists or criminals for purposes inconsistent with the objective of maintaining international stability and security, and it is therefore necessary to prevent their use for criminal or terrorist purposes. For that reason, Bangladesh supports the adoption of General Assembly resolution 61/54.

* A/62/150.



Brunei Darussalam

The following information was received from the Government of Brunei Darussalam in addition to the information already included in document A/62/98.

[Original: English]
[29 August 2007]

1. Key points

General appreciation of the issues of information security

1. The Authority for the Information and Communications Technology Industry (AITI) of Brunei Darussalam and the Brunei Ministry of Communications are appreciative of the ongoing work of the United Nations in promoting the importance of information security at the international level. We support continued international discussions on this issue in order to stimulate further international cooperation in this respect.

Efforts taken at the national level to strengthen information security and promote international cooperation in this field

2. In Brunei, we have legislation in place since 2000 making it a criminal offence to misuse computers and other related telecommunications equipment. We have also set up the National Computer Emergency Response Team (BruCERT) in 2004 to coordinate national responses to information security threats and to cooperate with the Asia Pacific Computer Emergency Response Team at the regional level.

Possible measures that could be taken by the international community to strengthen information security at the global level

3. AITI feels that the existence of computer security incident response teams (CSIRTs) operating at the national, regional and international levels is adequate to address the need to respond to information security threats. The methodology applied in compromising systems may just as easily be applied by warring Member States or terrorist organizations as they are by criminal organizations.

2. General appreciation of the issues of information security

4. With the increasing pervasiveness of information technology in all aspects of civil and military fields, AITI is mindful of the need to increase awareness at the national and international levels as to the sensitivity of information security risks.

3. Efforts taken at the national level

Legislation developed in 2000

5. The Computer Misuse Order (2000) adopts a descriptive approach in defining computer "misuse". As such, it covers a wide range of misuse not only affecting Internet systems but also mobile telephones and other telecommunications devices.

6. As of the date of the present report (May 2007), the legislation has not yet been used in a criminal case to prosecute computer misuse.

Brunei National Computer Emergency Response Team

7. BruCERT was established in May 2004, in collaboration with AITI and the Ministry of Communications, to become the nation's first trusted one-stop referral agency in dealing with computer-related and Internet-related security incidents in Brunei Darussalam.

8. This is in line with commitments made at the APECTEL Work Group level to facilitate international collaboration.

9. BruCERT coordinates with local and international CSIRTs, network service providers, security vendors, Government agencies and other related organizations to facilitate the detection, analysis and prevention of security incidents on the Internet.

4. Possible measures to strengthen information security

10. Because of the transboundary nature of attacks on information systems, AITI suggests that the existing network of CSIRTs is an appropriate mechanism for the international dissemination of information and knowledge-sharing.

11. Unlike "traditional" means of warfare, compromising national security by manipulating information system aspects does not require the manufacturing or acquisition of war machinery or weapons of mass destruction. Accordingly, the existing network of CSIRTs should be sufficient measures against coordinated cross-border network attacks.

12. In the Brunei context, the existing methods for cross-border prosecution for criminal offences would apply to crimes punishable under the Computer Misuse Order (2000). Therefore, AITI emphasizes that international cooperation is essential in order to prosecute information security criminals.